IN THE CLAIMS:

The following is a complete listing of the claims in this application, reflects all changes currently being made to the claims, and replaces all earlier versions and all earlier listings of the claims:

Claim 1 (Currently Amended): A method for cryptographing information between a client terminal and~~, which is executed in~~ a server which are connected to each other ~~connectable to a terminal of a client~~ through a network, the method comprising the steps of:

[[a)]] generating, at the server, a public key, a private encryption key ~~and a public key for information encryption~~ by driving an encryption module for encryption information to an access request from the client terminal;

[[b)]] sending, at the server, to the client terminal the ~~generated~~ public key and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and a double security by being included in a Web document for user input in the form of a Java applet ~~to the client terminal~~;

~~c) executing the encryption execution module and the public key in the client terminal to encrypt the information and receiving the encrypted information from the client terminal~~ sending, at the client terminal, to the server an encryption message including a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent form the server and a digest message digesting the original message, and including an encryption compression key encrypted with the public key; and

~~d) calling the generated private encryption key and decrypting the received encrypted information with the called private encryption key~~ upon receipt of the encryption message from the client terminal, decrypting, at the server, the encryption compression key by calling the private encryption key, decompressing the compressed result with the decrypted encryption compression key, and decrypting the original message with the private encryption key according to a result of the integrity verification.

Claim 2 (Currently Amended): The method as set forth in claim 1, wherein ~~the encrypted information is user authentication information required to log in~~ the original message decrypted with the private encryption key is user authentication information required to log in, and wherein the method further comprising the steps of:

[[e)]] comparing ~~the decrypted information with prestored information~~ at the server, the decrypted user authentication information with a previously stored user information database; and

[[f)]] allowing or denying, at the server, access of the client terminal to the server according to a result of information authentication.

Claim 3 (Currently Amended): The method as set forth in claim 1, wherein the ~~encrypted information is payment information~~ original message decrypted with the private encryption key is payment information and wherein the method further comprising the steps of:

[[e)]] sending, at the server, the decrypted payment information to a ~~connectable~~ financial payment institution server connected through a dedicated computer network; and

[[f)]] receiving, at the server, payment approval result information from the financial payment institution server and sending the received payment approval result information to the client terminal ~~the received payment approval result information~~;

Claim 4 (Currently Amended): The method as set forth in any one of claims 1 to 3, wherein the public key is generated by calculating coordinates of a point on an elliptic curve with a private encryption key value of n bits generated randomly by driving the encryption module and an elliptic curve initialization value.

Claim 5 (Currently Amended): The method as set forth in any one of claims 1 to 3, wherein the ~~step d) includes~~ the integrity verification is processed by the following steps of:

~~d-1) decrypting an encryption compression key contained in the encrypted information with the called private encryption key;~~

~~d-2) decompressing an original message and a digest message with the decrypted encryption compression key;~~

[[d-3)]] digesting, at the server, the decompressed original message; and

[[d-4)]] comparing, at the server, the digested original message with the decompressed digest message from the client terminal, and[[,]] if the digested original message and the decompressed digest are the same, decrypting the decompressed original message with the private encryption key.

Claim 6 (Currently Amended): A method for cryptographing information~~, which is executed in a computer connectable to~~ between a gateway communicating with ~~at least one~~ a

wireless terminal and a computer connected to the gateway, the method comprising the steps of:

[[a)]] generating, at the computer, a public key and a private encryption key ~~and a public key for information encryption~~ by driving an encryption module for information encryption according to an access request from the wireless terminal through the gateway;

[[b)]] sending, at the computer, ~~the generated~~ to the wireless terminal through the gateway public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security by being included in a Web document for user input in the form of a Java applet ~~to the wireless terminal~~;

~~c) executing the encryption execution module and the public key in the wireless terminal to encrypt the information and receiving the encrypted information from the wireless terminal through the gateway~~ sending, at the wireless terminal, to the computer through the gateway an encryption message including a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent from the computer and a digest message digesting the original message, and including an encryption compression key encrypted with the public key; and

~~d) calling the generated private encryption key and decrypting the received encrypted information with the called private encryption key~~ upon receipt of the encryption message from the wireless terminal through the gateway, decrypting, at the computer, the encryption compression key by calling the private encryption key, decompressing the compressed result with the decrypted encryption compression key, and decrypting the original message with the private encryption key according to a result of the integrity verification.

Claim 7 (Currently Amended): The method as set forth in claim 6, wherein the ~~step d) includes~~ integrity verification is processed by the steps of:

~~d-1) decrypting an encryption compression key contained in the encrypted information with the called private encryption key~~ digesting, at the computer, the decompressed original message; and

~~d-2) decompressing an original message and a digest message contained in the encrypted information with the decrypted encryption compression key;~~

~~d-3) digesting the decompressed original message; and~~

[[d-4)]] comparing, at the computer, the digested original message with the decompressed digest message from the wireless terminal through the gateway, and[[,]] if the digested original message and the decompressed digest message are the same, decrypting the

decompressed original message with the private encryption key.

Claim 8 (Currently Amended): A method for cryptographing information~~, which is downloaded together with a public key from~~ between a wired/wireless client terminal and an encryption server, which is ~~through a network and~~ executed in a wired/wireless terminal ~~of a client~~, the method comprising the steps of:

~~a) encrypting the information entered from a client with the public key to generate an original message~~ accessing the encryption server;

~~b) digesting the encrypted original message~~ downloading a public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security from the encryption server in a non-installed manner;

encrypting information entered from a client with the public key by executing the downloaded encryption execution module to generate an original message;

digesting the encrypted original message by the message digest module;

[[c)]] compressing the original message and the digested original message with an encryption compression key ~~under the condition that the encryption compression key is~~ generated by randomly extracting a part of the public key;

[[d)]] encrypting the encryption compression key with the public key having been used to encrypt the original message; and

[[e)]] converting the compressed original message, the compressed digested original message and the encrypted encryption compression key into a Web ~~documents~~ document file, and sending the Web ~~documents~~ document file to the encryption server.